

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

1300 I STREET, N. W.  
WASHINGTON, DC 20005-3315

202 • 408 • 4000  
FACSIMILE 202 • 408 • 4400

ATLANTA  
404 • 653 • 6400  
PALO ALTO  
650 • 849 • 6600

WRITER'S DIRECT DIAL NUMBER:



ATTORNEY DOCKET NO. 04329.2191

Assistant Commissioner  
for Patents  
Washington, D.C. 20231

TOKYO  
011 • 813 • 3431 • 6943  
BRUSSELS  
• 322 • 646 • 0353

TECH CENTER 2700

JAN 18 2000

RECEIVED

U.S. Patent Application for  
ENCRYPTION APPARATUS, CRYPTOGRAPHIC COMMUNICATION SYSTEM, KEY  
RECOVERY SYSTEM, AND STORAGE MEDIUM

Inventors: Akito NIWA et al.  
Serial No.: 09/448,470  
Filed: November 24, 1999

Group Art Unit: 2766

CLAIM FOR PRIORITY

Sir:

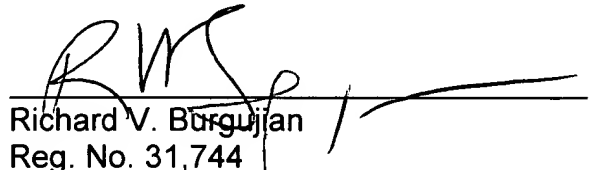
Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 10-334485 filed November 25, 1998, for the above identified United States Patent Application.

In support of applicants' claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW  
GARRETT & DUNNER, L.L.P.

by:

  
Richard V. Burguijan  
Reg. No. 31,744

Dated: 1/13/00

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日

Date of Application:

1998年11月25日

出願番号

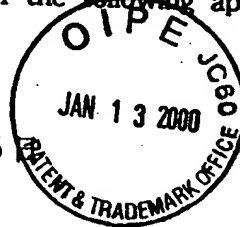
Application Number:

平成10年特許願第334485号

願人

Applicant(s):

株式会社東芝



TECH CENTER 2700

JAN 18 2000

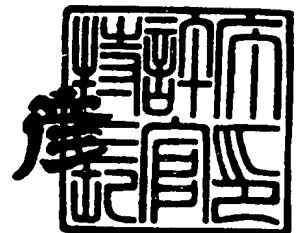
RECEIVED

CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年11月26日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



【書類名】 特許願

【整理番号】 A009805588

【提出日】 平成10年11月25日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00

【発明の名称】 暗号装置、暗号通信システム及び鍵復元システム並びに  
記憶媒体

【請求項の数】 6

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 才所 敏明

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 川村 信一

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 堀 智美

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 青木 恵

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 石原 達也

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 佐野 文彦

【発明者】

    【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

    【氏名】 丹羽 朗人

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体

【特許請求の範囲】

【請求項 1】 データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置であって、

暗号化したデータ本体を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データと、

暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データとを前記送信データに含める手段を備えたことを特徴とする暗号装置。

【請求項 2】 前記送信者又は前記受信者が複数の鍵復元者に登録している場合に、

前記送信者又は前記受信者鍵復元データに含まれる復元用情報は、暗号化データ本体を復号する復号鍵の部分の集合であり、各復号鍵の部分はそれぞれ異なる鍵復元者に復号可能に暗号化されることを特徴とする請求項 1 記載の暗号装置。

【請求項 3】 前記請求項 1 又は 2 記載の暗号装置と、

送信者又は受信者が自己に登録している場合には、その送信者又は受信者鍵復元データを復号可能とする鍵復号者装置と、

少なくとも前記鍵復元者及び前記受信者の認証局登録を受け付け可能に構成されると共に、登録された各受信者が何れの鍵復元者に登録しているかの情報、並びに前記暗号装置が前記復元用情報を鍵復元者に復号可能に暗号化するための情報とを提供可能に構成された認証局装置とを備えたことを特徴とする暗号通信システム。

【請求項 4】 前記鍵復元者に対する登録承認を要求する者に承認を与えると共に、前記送信者又は前記受信者鍵復元データの復号承認を要求する正当権限者に対し、前記送信者又は前記受信者鍵復元データの復号承認を与える承認者装置を備え、

前記鍵復号者装置は、前記承認者の承認を得ている者から依頼された場合にのみ、前記送信者又は前記受信者鍵復元データを復号して返送することを特徴とする請求項3記載の暗号通信システム。

【請求項5】 データを暗号化又は復号するために鍵情報を用いると共に、前記鍵情報を復元するための復元用情報を、自己が登録している鍵復元者に復号可能に暗号化した状態で前記鍵情報と別途に保存する暗号装置と、

前記鍵復元者に対する登録承認を要求する者に承認を与えると共に、暗号化された前記復元用情報の復号承認を要求する正当権限者に対し、前記暗号化された復元用情報の復号承認を与える承認者装置と、

前記承認者の承認を得ている者から復号を依頼された場合にのみ、前記暗号化された復元用情報を復号して返送する鍵復号者装置とを備えたことを特徴とする鍵復元システム。

【請求項6】 データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置を制御するプログラムであって、

暗号化させたデータ本体を復号させる鍵を復元させるための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化させた送信者鍵復元データと、

暗号化させたデータ本体を復号させる鍵を復元させるための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化させた受信者鍵復元データと

を前記送信データに含めさせる手段を有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は暗号及び復号処理に用いる暗号鍵及び復号鍵の管理の部分に特徴のある暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体に関するものである。

【0002】

【従来の技術】

近年では、オープンなネットワーク上でデータ（メッセージ）通信を行う場合、データの盗聴及び改竄を防止するためにデータを暗号化するようになっている。

【0003】

このデータ暗号化のために暗号鍵が用いられるが、ユーザ自身による鍵の紛失や何らかの原因により鍵を破壊してしまう場合がある。また、状況に応じて正当な理由を持つ第三者が、暗号通信を傍受する必要性が生じる場合もある。これらの事態に対応するために、何らかの方式で鍵を復元できることが要求される。

【0004】

従来、提供されている鍵復元システムは、暗号通信の当事者が鍵復元処理を実際に行う鍵復元エージェントに予め登録をしておき、その登録に対応して復号可能とした鍵復元フィールドを暗号化データに付加することで実現される。この鍵復元フィールドは暗号化されているが、これを復号することで当該鍵（通信用の共通鍵等）が復元されるようになっている。

【0005】

すなわち、送受信者や正当権限を有する第三者は必要な場合には鍵復元フィールドを鍵復元エージェントに送信し、紛失等した鍵を復元してもらうようになっている。

【0006】

【発明が解決しようとする課題】

しかしながら、上記した従来の鍵復元方式では、鍵復元エージェントにとって鍵の復元要求者が正当な権限を有しているか否かを確認することが困難である。また、鍵復元エージェントが悪意の第三者と結託して不正な鍵復元を行うような場合を防止することはできない。

【0007】

さらに、データ通信における送信者と受信者とが異なる鍵復元エージェントに登録しているような場合、特に国際間における暗号通信の場合には、受信者



や正当権限第三者が登録している鍵復元エージェントでは送信者の鍵復元フィールドを復元することができない。例えば送信者がAという鍵復元エージェントに登録し、受信者がBという鍵復元エージェントに登録しており、受信者はAの存在がわからないような場合を考える。このとき、受信者が例えば暗号通信の共通鍵を紛失すると、暗号化データの鍵復元フィールドをBに送っても紛失した共通鍵は復元できない。また、送信者と受信者が異なる国の者であるような場合には、受信者はAの所在を知ることは容易ではない。正当権限第三者についても同様な事情が生じる。

## 【0008】

本発明は、このような実情を考慮してなされたもので、その第1の目的は、鍵復元に関する権限集中やエージェントの結託等の防止を可能として、鍵復元の安全性を高いものとすることができる暗号通信システム及び鍵復元システムを提供することにある。

## 【0009】

また、第2の目的は、異なるエージェントに登録するユーザ間で暗号化通信を行う場合でも、そのユーザあるいは正当権限を有する第三者が容易にエージェント情報を取得でき、鍵復元を行うことができる暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体を提供することにある。

## 【0010】

## 【課題を解決するための手段】

上記課題を解決するために、請求項1に対応する発明は、データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置であって、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データと、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データとを送信データに含める手段を備えた暗号装置である。

## 【0011】

本発明はこのような手段を設けたので、それぞれ異なる鍵復元者に登録する

送受信者間で暗号化通信を行う場合でも、その送受信者あるいは正当権限を有する第三者が容易に鍵復元を行うことができる。

【0012】

次に、請求項2に対応する発明は、請求項1に対応する発明において、送信者又は受信者が複数の鍵復元者に登録している場合に、送信者又は受信者鍵復元データに含まれる復元用情報は、暗号化データ本体を復号する復号鍵の部分の集合であり、各復号鍵の部分はそれぞれ異なる鍵復元者に復号可能に暗号化される暗号装置である。

【0013】

本発明はこのような手段を設けたので、鍵を復元するための情報の復号を、複数の鍵復元者に分散させて行わせることができ、鍵情報の秘匿安全性を高めることができる。

【0014】

次に、請求項3に対応する発明は、請求項1又は2に対応する暗号装置と、送信者又は受信者が自己に登録している場合には、その送信者又は受信者鍵復元データを復号可能とする鍵復号者装置と、少なくとも鍵復元者及び受信者の認証局登録を受け付け可能に構成されると共に、登録された各受信者が何れの鍵復元者に登録しているかの情報、並びに前記暗号装置が復元用情報を鍵復元者に復号可能に暗号化するための情報とを提供可能に構成された認証局装置とを備えた暗号通信システムである。

【0015】

本発明はこのような手段を設けたので、それぞれ異なる鍵復元者に登録する送受信者間で暗号化通信を行う場合でも、その送受信者あるいは正当権限を有する第三者が容易に鍵復元者についての情報を取得することができ、かつ容易に鍵復元を行うことができる。さらに、鍵復号に関する権限集中や鍵復元者と悪意の者との結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【0016】

次に、請求項4に対応する発明は、請求項3に対応する発明において、鍵復

元者に対する登録承認を要求する者に承認を与えると共に、送信者又は受信者鍵復元データの復号承認を要求する正当権限者に対し、送信者又は受信者鍵復元データの復号承認を与える承認者装置を備え、鍵復号者装置は、承認者の承認を得ている者から依頼された場合にのみ、送信者又は受信者鍵復元データを復号して返送する暗号通信システムである。

【0017】

本発明はこのような手段を設けたので、鍵復元者と悪意の者との結託等の防止が一層強化され、鍵復元の安全性をより高いものとすることができる。

【0018】

次に、請求項5に対応する発明は、データを暗号化又は復号するために鍵情報を用いると共に、鍵情報を復元するための復元用情報を、自己が登録している鍵復元者に復号可能に暗号化した状態で鍵情報と別途に保存する暗号装置と、鍵復元者に対する登録承認を要求する者に承認を与えると共に、暗号化された復元用情報の復号承認を要求する正当権限者に対し、暗号化された復元用情報の復号承認を与える承認者装置と、承認者の承認を得ている者から復号を依頼された場合にのみ、暗号化された復元用情報を復号して返送する鍵復号者装置とを備えた鍵復元システムである。

【0019】

本発明はこのような手段を設けたので、あらゆる種類の鍵情報の復元を可能とすると共に、鍵復号に関する権限集中や鍵復元者と悪意の者との結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【0020】

次に、請求項6に対応する発明は、請求項1に対応する発明をコンピュータに実現させるプログラムを記憶した記憶媒体である。

【0021】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項1の暗号装置として機能する。

【0022】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【0023】

図1は本発明の実施の形態に係る暗号通信システムの全体構成例を示す構成図である。

【0024】

この暗号通信システムは、ユーザ1間で暗号化通信を行う場合に、そのセッション鍵やユーザ秘密鍵を復元可能とするために、鍵復元エージェント3、認証局2及び承認者4を設けてなるものである。ユーザ1、鍵復元エージェント3、認証局2及び承認者4の間は公衆回線等からなるネットワーク（インターネット等）で通信可能に構成されている。

【0025】

図2は本実施形態のユーザ1、鍵復元エージェント3、認証局2（鍵復元センタ）又は承認者4を構成する装置のハードウェア構成例を示すブロック図である。

【0026】

ユーザ1、鍵復元エージェント3、認証局2又は承認者4を構成する装置11は、ハードウェア的には、CPU12、コントローラ13、メモリ14、通信デバイス15、ディスプレイ16、キーボード17、プリンタ18及びデータバス19より構成される計算機システムである。

【0027】

これらの構成のうち、メモリ14は、いわゆる主記憶（RAM等）と二次記憶装置（ハードディスク等）の双方を含むものである。この主記憶上に読み込まれたプログラムと、このプログラムに従うCPU12の制御によって、ユーザ1、鍵復元エージェント3、認証局2又は承認者4が行うべき機能が実現される。すなわちソフトウェア的には、ユーザ1、鍵復元エージェント3、認証局2又は承認者4は異なる構成を有するものである。これらハードウェア及びソフトウェアの結合からなるそれぞれの機能の詳細な内容については、後述する動作説明において流れ図により説明する。

【0028】

また、メモリ 14 の二次記憶装置の部分には、ユーザ 1、鍵復元エージェント 3、認証局 2 又は承認者 4 それぞれに対応して、通信メッセージや各種証明書、公開鍵、各種情報リスト等が格納され、各機能の実現に際して使用される。

【0029】

さらに、通信デバイス 15 は、ネットワークに接続され、CPU 12 の制御によって、各種の情報を送受する。

【0030】

次に、ユーザ 1、鍵復元エージェント 3、認証局 2 又は承認者 4 について説明する。

【0031】

ユーザ 1 は、暗号メッセージ（暗号通信）の送信者、受信者あるいは当該暗号メッセージを傍受する正当権限を有する第三者を示している。図 1 では、ユーザ 1（＃1）を送信者、ユーザ 1（＃2）を受信者、ユーザ 1（＃3）を正当権限第三者としている。また、ユーザ 1 は、送信者、受信者及び正当権限第三者に必要な全ての機能を備えており、状況によって、これらの何れかになる。

【0032】

具体的には、ユーザ 1 は、自己の公開鍵、秘密鍵を有すると共に、鍵復元エージェント 3 の登録機能、暗号メッセージ作成機能、メッセージ送受信機能、暗号メッセージ復号機能及び鍵の復元要求・復元機能等を備えている。なお、図 2 の装置 11 は、ユーザ 1 の暗号装置を構成するものである。

【0033】

鍵復元エージェント 3 は、自己の公開鍵と秘密鍵を有し、登録されたユーザ 1 からの要求に応じ、受信した鍵復元フィールドを自己の秘密鍵で復号して返信するものである。これらの処理を行うに際し、登録時の承認者 4 の署名を確認するようになっている。また、鍵復元エージェント 3 は、多数存在することが可能で、認証局 2 への登録により、ある者は本実施形態でいう鍵復元エージェント 3 となる。本実施形態では、鍵復元エージェント 3（＃1）～3（＃n

）が存在する。

【0034】

認証局 2 は、自己の公開鍵及び秘密鍵を有すると共に、各ユーザ 1、各鍵復元エージェント 3、各承認者 4 についての公開鍵に署名（認証）を与え、各種の証明書を発行すると共に、これらの情報をユーザ 1 等に開放するものである。

【0035】

承認者 4 は、ユーザ 1 が鍵復元エージェントに登録したり鍵復元要求を行う場合等に当該ユーザ 1 に承認書を発行するものである。この承認者 4 も多数存在することが可能であり、本実施形態では、承認者 4（#1）～4（#m）が存在する。なお、ユーザ 1 が複数の承認者 4 から 1 つの承認をもらうことも可能であり、このような場合には、代表承認者が設けられる。

【0036】

次に、以上のように構成された本実施形態における暗号通信システム及び暗号装置の動作について説明する。

【0037】

この暗号通信システムにおいては、まず鍵復元エージェントが認証局に自己の公開鍵に登録し、鍵復元を望むユーザは、認証局に登録された何れかの鍵復元エージェントから鍵復元要求を行うエージェントを選択して予め登録する。

【0038】

このような準備の後、ユーザ間通信が行われ、鍵紛失等により通信用のセッション鍵やユーザ秘密鍵を復元する必要があるときには、登録したエージェントに鍵復元を依頼する。

【0039】

以下、本システムの動作について、登録、通信及び鍵復元のそれぞれについて説明する。

（鍵復元エージェントの登録手続き）

図 3 は鍵復元エージェントの認証局への登録手続処理を示す流れ図である。

【0040】

まず、認証局2への登録を望む鍵復元エージェント3は、自己の公開鍵と公開鍵に対する自分の署名を含む登録申請書を認証局2へ送信する（図3：s1，図1：a）。

【0041】

認証局2はこの鍵復元エージェント3についての調査や署名確認等を行った後（図3：s2）、当該鍵復元エージェント3に対し、鍵復元エージェント3の公開鍵を含む申請データに認証局の署名を付加した公開鍵証明書17を発行する（図3：s3，図1：b）。

【0042】

こうして登録された鍵復元エージェント3については、認証局2にてユーザ／承認者／鍵復元エージェントの登録情報テーブルに登録され、この登録情報テーブルの内容はユーザ1等に開放される。以下、鍵復元エージェント3というときは、認証局2に登録されたエージェントを意味する。

（ユーザの登録手続き）

次に、メッセージ通信を行いたいユーザ1は、鍵復元エージェントを選択し、自己が何れの鍵復元エージェント3を利用するかについて、認証局2に登録を行う。

【0043】

図4はユーザの鍵登録エージェント登録手続処理を示す流れ図である。

【0044】

ここでは図1のユーザ1（#1）が登録を行う場合について説明する。

【0045】

まず、ユーザ1（#1）は、一又は複数の鍵復元エージェント3への加入に際し、まず承認者4に対し、鍵復元エージェント登録申請18を行う（図4：t1，図1：c）。

【0046】

ユーザ1は、一の承認者4に対して承認を求めるようにしてもよいが、鍵復元に関する安全性を高めるために複数の承認者4に承認を求めるようにしてもよい。複数の承認者4に承認を求める場合には、ユーザ1は代表承認者のみに

登録申請を行う（図4：t1）。

【0047】

代表承認者は各承認者4に登録申請書を回付し、各承認者4は鍵復元エージェント登録申請内容を検査し署名を施す（例えば、多重署名方式を用いる）。申請書は、最後に代表承認者に戻され、当該代表承認者からユーザ1（#1）に鍵復元エージェント登録承認書が送信される（図4：t2，図1：d）。

【0048】

次に、ユーザ1（#1）は自己が登録を希望する各鍵復元エージェント3に対し、承認者4から取得した鍵復元エージェント登録承認書を添付して加入申請を行う（図4：t3，図1：e）。なお、ユーザ1が登録する鍵復元エージェント3は、一つでもよいが、本実施形態では原則として複数の鍵復元エージェント3に登録する場合で説明する。

【0049】

登録承認書を受けた各鍵復元エージェント3は鍵復元エージェント登録承認書における承認者4の署名を検証し、自身の署名を付加し、ユーザ1（#1）に対し鍵復元エージェント登録証明書を発行する（図4：t4，図1：f）。

【0050】

次に、全ての鍵復元エージェント3について鍵復元エージェント登録証明書の取得処理が終了していなければ、ステップt1～t4の処理を繰り返す（図4：t5）。

【0051】

次に、ユーザ1（#1）は認証局2に対し、エージェント3から取得した鍵復元エージェント登録証明書を添付して登録鍵復元エージェントリスト証明書の発行申請を行う（図4：t6，図1：g）。

【0052】

認証局2はこの鍵復元エージェント登録証明書における鍵復元エージェント4による署名を検証し、自身の署名を付加し、ユーザ1（#1）に対し登録鍵復元エージェントリスト証明書を発行する（図4：t7，図1：h）。

【0053】



このエージェントリストにリストアップされた鍵復元エージェント 3 がユーザ 1（# 1）の登録鍵復元エージェント 3 であり、ユーザ 1（# 1）用の鍵復元フィールドは、これらのエージェント 3 の有する秘密鍵で解読可能となる。

【0054】

なお、認証局 2 は、登録鍵復元エージェントリスト証明書を発行すると共に、同リストの内容を上記登録情報テーブルに反映させる。

【0055】

図 5 は認証局に設けられた登録情報テーブルの構成例を示す図である。

【0056】

同図に示すように、登録情報テーブル 21 には、ユーザ 1，承認者 4 又は鍵復元エージェント 3 のユーザ ID（識別情報）22 に対応して、認証局がその者の公開鍵として認証した署名付き公開鍵 23 と、ユーザ登録エージェントリスト 24 とが設けられている。

【0057】

署名付き公開鍵 23 は、その鍵が当該ユーザ 1 等の公開鍵であることを認証局が証明するものであり、公開鍵証明書の形で当該情報の要求者に発行される。

【0058】

ユーザ登録エージェントリスト 24 は、各登録ユーザのみに対応して設けられ、このリスト内容の発行を受けることで、第三者は当該ユーザ 1 がどの鍵復元エージェント 3 に登録しているかを知ることができる。

【0059】

なお、この登録情報テーブル 21 の内容は一般に公開されており、ユーザ 1 やエージェント 3 等はあたかも電話帳を調べるような形でその内容を知ることができる。また、テーブル 21 に登録されたエージェント 3 は、自己の公開鍵を認証局 2 に登録しており、これらの公開鍵はテーブル 21 上に掲載してもよい。

（暗号化メッセージの送受信処理）

次に、このようなエージェント登録を行ったユーザ 1 間で、実際に暗号化メ

ッセージを送受信するときの処理を説明する。なお、この場合は、ユーザ 1（# 1）が送信者となり、ユーザ 1（# 2）が受信者となる場合を説明する。ユーザ 1（# 2）も図 4 に示す処理によりエージェント登録を行っているものとする。

#### 【0060】

図 6 は暗号化メッセージの送受信処理を示す流れ図である。

#### 【0061】

図 7 は暗号化メッセージの送受信を行う場合のユーザ及び認証局の関係を示す図である。

#### 【0062】

まず、送信者であるユーザ 1（# 1）（以下、単に送信者ともいう）は、受信者であるユーザ 1（# 2）（以下、単に受信者ともいう）が登録している鍵復元エージェント 3 の情報を得るために、認証局 2 へ受信者の公開鍵と登録鍵復元エージェントリストの照会を行う（図 6：v 1，図 7：i）。

#### 【0063】

認証局 2 は、登録情報テーブル 2 1 の内容から受信者の公開鍵証明書と登録鍵復元エージェントリスト証明書を作成し、送信者に送信する（図 6：v 2，図 7：j）。この処理は、ユーザ 1 が認証局 2 に設けられた電話帳（登録情報テーブル 2 1）を調べる行為に相当する。

#### 【0064】

次に、送信者は、認証局 2 から入手した受信者の登録鍵復元エージェントリスト証明書を利用して送信メッセージ（暗号化メッセージ）を作成する（図 6：v 3）。

#### 【0065】

図 8 は送信者が作成する暗号化メッセージのデータ構造例を示す図である。

#### 【0066】

この暗号化メッセージ 3 1 は、ヘッダ 3 2 と、送信側鍵復元フィールド 3 3 と、受信側鍵復元フィールド 3 4 と、署名 3 5 と、セッション鍵配送情報 3 6 と、暗号化メッセージ本体 3 7 とから構成される。

【0067】

ここでまずヘッダ32には、送信側及び受信側鍵復元フィールド等の後続するデータのサイズ等の情報が格納される。

【0068】

送信側鍵復元フィールド33には、送信者側の鍵復元エージェント3が鍵を復元する際に用いる情報が格納され、受信側鍵復元フィールド34には、受信者側の鍵復元エージェント3が鍵を復元する際に用いる情報が格納される。送信側及び受信側鍵復元フィールド33, 34には、鍵復元エージェント3のID38と、鍵復元エージェント3の公開鍵で暗号化したセッション鍵又はセッション鍵ピース $[[Ski] KRA(i)pb]$ のデータ39との組が鍵復元エージェント数だけ格納される。

【0069】

なお、受信側鍵復元フィールド34を作成するために用いる受信者のエージェントID及びエージェント公開鍵は、ステップv2で入手した登録鍵復元エージェントリスト証明書から取得する。

【0070】

また、暗号化メッセージ31には、送信側及び受信側鍵復元フィールド $[KRF]$ 33, 34の改竄防止のために、送信者の鍵 $[USR1pr]$ を用いて生成した署名35 $([[KRF] USR1pr])$ が付加されている。

【0071】

セッション鍵配送情報36には、受信者の公開鍵 $[USR2pb]$ で暗号化したセッション鍵 $[[SK] USR2pb]$ が格納される。

【0072】

暗号化メッセージ31の最後には、送信データの本体として、セッション鍵 $[SK]$ で暗号化した暗号化メッセージ本体37 $([[M] SK])$ が付加されている。

【0073】

さて、このように構成された暗号化メッセージ31は、送信者（ユーザ1（#1））から受信者（ユーザ1（#2））に送信される（図6：v4，図7：

k)。

【0074】

受信者は、図8に示す構造の暗号化メッセージを受け取ると、自己の秘密鍵を用いてセッション鍵情報36を復号してセッション鍵を取り出し、さらに、そのセッション鍵を用いて暗号化メッセージ本体37を復号して送信データを取り出す(図6:v5)。

(セッション鍵の鍵復元手続き)

上記図6のステップv5のように正常に暗号化メッセージを復号できた場合には特に問題は生じない。ここでは、ユーザ1がセッション鍵を紛失したような場合の復元処理について説明する。

【0075】

図9は送信者又は受信者による鍵復元手続処理を示す流れ図である。

【0076】

図10は送信者又は受信者による鍵復元手続のユーザ、鍵復元エージェント及び承認者の関係を示す図である。

【0077】

ここではまず、鍵復元を依頼するユーザ1が、復元対象となる鍵復元フィールドを復元可能な鍵復元エージェント3に関する情報(ID等)を予め有している場合について説明する。このような場合は、ユーザ1がメッセージの送信者(ユーザ1(#1))である場合や受信者(ユーザ1(#2))である場合である。

【0078】

ここでは、受信者がセッション鍵を何らかの理由で取得できなくなり、暗号化メッセージ本体37を読めなくなってしまった場合について説明する。

【0079】

ユーザ1(#2)は、セッション鍵を紛失等した場合(図9:w1)、まず、承認者4に対し鍵復元承認申請書を送信する(図9:w2, 図10:1)。

【0080】

承認者4は鍵復元承認申請書を検査した後、署名を施し(例えば、多重署名

方式を用いる)、代表承認者から鍵復元承認書をユーザ 1 (#2) へ送信する (図 9:w3, 図 10:m)。

【0081】

次に、ユーザ 1 (#2) は、暗号化メッセージ 32 から鍵復元フィールド 33 又は 34 を取り出し、鍵復元フィールドに指定されている各鍵復元エージェント 3 へ対するメッセージを作成する (図 9:w4)。

【0082】

図 11 はユーザが鍵復元エージェントに送信するメッセージのデータ構造例を示す図である。

【0083】

同図に示すように、このメッセージ 41 は、承認者 4 から得た鍵復元承認書 42 と、暗号化メッセージ 31 から取り出した鍵復元フィールド 43 と、復元したセッション鍵ピースを送信する際に用いる暗号鍵 44 とから構成されるデータ  $[M']$  を、各鍵復元エージェントの公開鍵  $[KRA(i)pb]$  で暗号化してなるものである。

【0084】

ユーザ 1 (#2) は、承認書 42 及び復元フィールド 43 を含むこのメッセージ 41 を各鍵復元エージェント 3 に送信する (図 9:w5, 図 10:n)。

【0085】

鍵復元エージェント 3 は暗号化された  $[[M'] KRA(i)pb] 41'$  を自己の秘密鍵で復号して鍵復元承認書、鍵復元フィールド及び暗号鍵  $[SK']$  を取り出し、鍵復元承認書 42 における承認者の署名を検証する (図 9:w6)。

【0086】

承認書 42 の確認の後、鍵復元エージェント 3 は、鍵復元フィールド 43 を自己の秘密鍵で復号し、セッション鍵のピースを復元する (図 9:w7)。この復元したピースは、暗号鍵  $[SK'] 44$  で暗号化され、エージェント 3 からユーザ 1 (#2) へ送信される (図 9:w7, 図 10:o)。

【0087】

このセッションピースを受け取ったユーザ 1（# 2）は、各鍵復元エージェント 3 から送信された暗号化されたセッション鍵のピースを暗号鍵 [SK'] 44 で復号する。さらに、例えばラグランジュ補間多項式を用い、復号されたセッション鍵のピースをもとに元のセッション鍵を復元する（図 9 : w 7）。

【0088】

なお、ラグランジュ補間多項式を用いるのは、複数のピースのうち一定数以上のピースが復元できれば、セッション鍵を復元できるようにするためである。つまり、ラグランジュ補間多項式を用いて鍵をピースに分散した場合、n 個に分散した鍵ピースから所定の k ( $\leq n$ ) 個だけ集めるだけで鍵を復元できるものである。

【0089】

次に、鍵復元を依頼するユーザ 1 が、復元対象となる鍵復元フィールドを復元可能な鍵復元エージェント 3 に関する情報 (ID 等) を有していない場合について説明する。このような場合は、ユーザ 1 が正当権限を有する第三者 (ユーザ 1 (# 1)) のような場合が考えられる。

【0090】

図 12 は第三者による鍵復元手続処理を示す流れ図である。

【0091】

この場合には、まず、暗号化メッセージ 31 に含まれる鍵復元フィールド 33 又は 34 についての鍵復元エージェント 3 の情報を取得する必要がある。

【0092】

このためにまず、ユーザ 1 (# 3) は認証局 2 へ送信者又は受信者の公開鍵と登録鍵復元エージェントリストの照会を行う（図 12 : x 1）。

【0093】

認証局 2 は、登録情報テーブル 21 の内容から送信者又は受信者の公開鍵証明書と登録鍵復元エージェントリスト証明書を作成しユーザ 1 に送信し、ユーザ 1 (# 3) はこれを受信する（図 12 : x 2）。この処理は、ユーザ 1 (# 3) が認証局 2 に設けられた電話帳（登録情報テーブル 21）を調べる行為に相当する。

## 【0094】

以下、ユーザ1（＃3）は、承認者4に鍵復元のための承認を求め（図1：p，q）、その承認書を復号対象の鍵復元フィールドとともに鍵復元エージェント3に送付して復元ピースを受領し（図1：r，s）、さらにはセッション鍵を復元することになる。この処理は図11のステップww（w2～w8）と同様であるので詳細説明は省略する。

## （他の鍵の鍵復元手続き）

上記場合は、暗号通信に含まれるセッション鍵そのものの復元について説明したが、本実施形態のシステムを用いれば他の鍵の復元も可能である。この他の鍵として、ユーザ1等が用いる秘密鍵（ユーザ秘密鍵）の場合でその復元処理を説明する。なお、この場合には、本実施形態は、鍵復元システムとして動作する。

## 【0095】

図13は鍵復元手続におけるユーザ、鍵復元エージェント及び承認者の関係を示す図である。

## 【0096】

ユーザ1（＃1）は、自身の秘密鍵を鍵復元エージェント3の公開鍵で暗号化（登録エージェントが一つの場合）、または秘密鍵をピースに分割し（登録エージェントが複数の場合、以下この場合で説明する）、各々のピースに対し異なる鍵復元エージェント3の公開鍵で暗号化したユーザ秘密鍵復元フィールドを生成し、秘密鍵のバックアップとしてユーザが所有する記憶装置に保存しておく。このユーザ秘密鍵復元フィールドは、図8における送信側又は受信側鍵復元フィールドに相当する。

## 【0097】

ユーザ秘密鍵復元フィールドには、鍵復元エージェントのIDと鍵復元エージェントの公開鍵で暗号化した秘密鍵又は暗号化した秘密鍵ピースのデータが鍵復元エージェント数だけ格納されている。秘密鍵が何らかの原因で紛失または破壊され、ユーザ自身で復元できなくなった場合に、ユーザ1（＃1）は承認者4に対しユーザ秘密鍵復元承認申請を行う（図13：t）。各承認者4は

ユーザ秘密鍵復元承認申請を検査し署名を施し（例えば多重署名を用いる）、最後の承認者（代表承認者）からユーザ秘密鍵復元承認書をユーザ 1（＃ 1）に送信する（図 13 : u）。

【0098】

次に、ユーザ 1（＃ 1）は各鍵復元エージェント 3 へ、各鍵復元エージェントの公開鍵で暗号化したユーザ秘密鍵復元承認書、ユーザ秘密鍵復元フィールド及び復元したユーザ秘密鍵またはユーザ秘密鍵ピースを送信する際に用いる暗号鍵を送信する（図 13 : v）。このとき送信するデータは図 11 に示すものと同様なものである。

【0099】

各鍵復元エージェント 3 は、暗号化されたユーザ秘密鍵復元承認書、ユーザ秘密鍵復元フィールド及び復元したユーザ秘密鍵ピース（又はユーザ秘密鍵）を送信する際に用いる暗号鍵を復号し、ユーザ秘密鍵復元承認書における承認者の署名検証する。その後、ユーザ秘密鍵復元フィールドを用いて各々の鍵復元エージェントが秘密鍵のピース（又は秘密鍵全体）を復元し、ユーザが指定した秘密鍵ピース送信用の暗号鍵を用いて暗号化した秘密鍵ピース（又は秘密鍵全体）をユーザ 1（＃ 1）に送信する（図 13 : w）。

【0100】

ユーザ 1（＃ 1）は、各鍵復元エージェント 3 から送信された暗号化された秘密鍵ピース（又は秘密鍵全体）を復号する。また、ピースを受け取った場合には、例えばラグランジュ補間多項式を用い、秘密鍵のピースに基づき元の秘密鍵を復元する。

【0101】

上述したように、本発明の実施の形態に係る暗号通信システム及び暗号装置は、鍵復元エージェント 3 の他、認証局 2 及び承認者 4 を設けるようにしたので、鍵復元エージェントの鍵復元に対する権力を分散化することができ、鍵復元の安全性を高いものとすることができる。

【0102】

また、鍵復元センター（認証局）や鍵復元エージェントによる鍵復元機能の



集中化を抑制するために、少なくとも一人以上で構成される承認者が、鍵復元エージェントに対するユーザ登録申請書、鍵復元申請書、秘密鍵復元申請書を検証及び承認するので、各種情報を管理する認証局2の他に、第三者的な承認者4による承認処理が導入され、鍵復元に関する安全性は特に高いものとなる。

【0103】

さらに、ユーザは、認証局に登録された複数の鍵復元エージェントから適宜選択しエージェント登録を行うことができるので、一層安全性、信頼性の高い鍵復元を実施することができる。また、鍵復元エージェントの悪意の者との結託等も防止できる。

【0104】

また、認証局2に登録情報テーブル21を設けてその情報を一般に開放するようにしたので、エージェントへの登録情報等を問い合わせることが容易であり、異なる鍵復元エージェント3に登録するユーザ間の暗号通信における鍵復元処理の容易に行うことができる。

【0105】

さらに、送信者が登録する鍵復元エージェントの情報が含まれている送信側鍵復元フィールドと、受信者が登録する鍵復元エージェントの情報が含まれている受信側鍵復元フィールドを生成し、暗号化データと共に送信するようにしたので、データ通信を行う送信者と受信者が異なる鍵復元センターの管轄下にある場合であっても鍵復元を容易に行うことができる。

【0106】

また、本実施形態の鍵復元システムによれば、暗号化データを生成する際に用いるセッション鍵の復元だけでなく、鍵配送や署名生成等に用いる秘密鍵についてもその鍵情報を複数の鍵復元エージェントを用いて復元することができる。

【0107】

なお、本発明は、記憶媒体に格納したプログラムやデータ等をコンピュータに読み込ませて実現することが可能であり、この記憶媒体としては、磁気ディ

スク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0108】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0109】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0110】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【0111】

なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0112】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0113】

【発明の効果】

以上詳記したように本発明によれば、鍵復号に関する権限集中やエージェン

トの結託等の防止を可能として、鍵復元の安全性を高いものとする事ができる暗号通信システム及び鍵復元システムを提供することができる。

【0114】

また、本発明によれば、異なるエージェントに登録するユーザ間で暗号化通信を行う場合でも、そのユーザあるいは正当権限を有する第三者が容易にエージェント情報を取得でき、鍵復元を行うことができる暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態に係る暗号通信システムの全体構成例を示す構成図。

【図2】

同実施形態のユーザ、復元エージェント、認証局又は承認者を構成する装置のハードウェア構成例を示すブロック図。

【図3】

鍵復元エージェントの認証局への登録手続処理を示す流れ図。

【図4】

ユーザの鍵登録エージェント登録手続処理を示す流れ図。

【図5】

認証局に設けられた登録情報テーブルの構成例を示す図。

【図6】

暗号化メッセージの送受信処理を示す流れ図。

【図7】

暗号化メッセージの送受信を行う場合のユーザ及び認証局の関係を示す図。

【図8】

送信者が作成する暗号化メッセージのデータ構造例を示す図。

【図9】

送信者又は受信者による鍵復元手続処理を示す流れ図。

【図10】

送信者又は受信者による鍵復元手続のユーザ、鍵復元エージェント及び承認

者の関係を示す図。

【図 1 1】

ユーザが鍵復元エージェントに送信するメッセージのデータ構造例を示す図

。

【図 1 2】

第三者による鍵復元手続処理を示す流れ図。

【図 1 3】

鍵復元手続におけるユーザ，鍵復元エージェント及び承認者の関係を示す図

。

【符号の説明】

1 …ユーザ

2 …鍵復元エージェント

3 …認証局

4 …承認者

1 1 …鍵復元エージェント，認証局又は承認者を構成する装置

1 2 …CPU

1 3 …コントローラ

1 4 …メモリ

1 5 …通信デバイス

1 6 …ディスプレイ

1 7 …キーボード

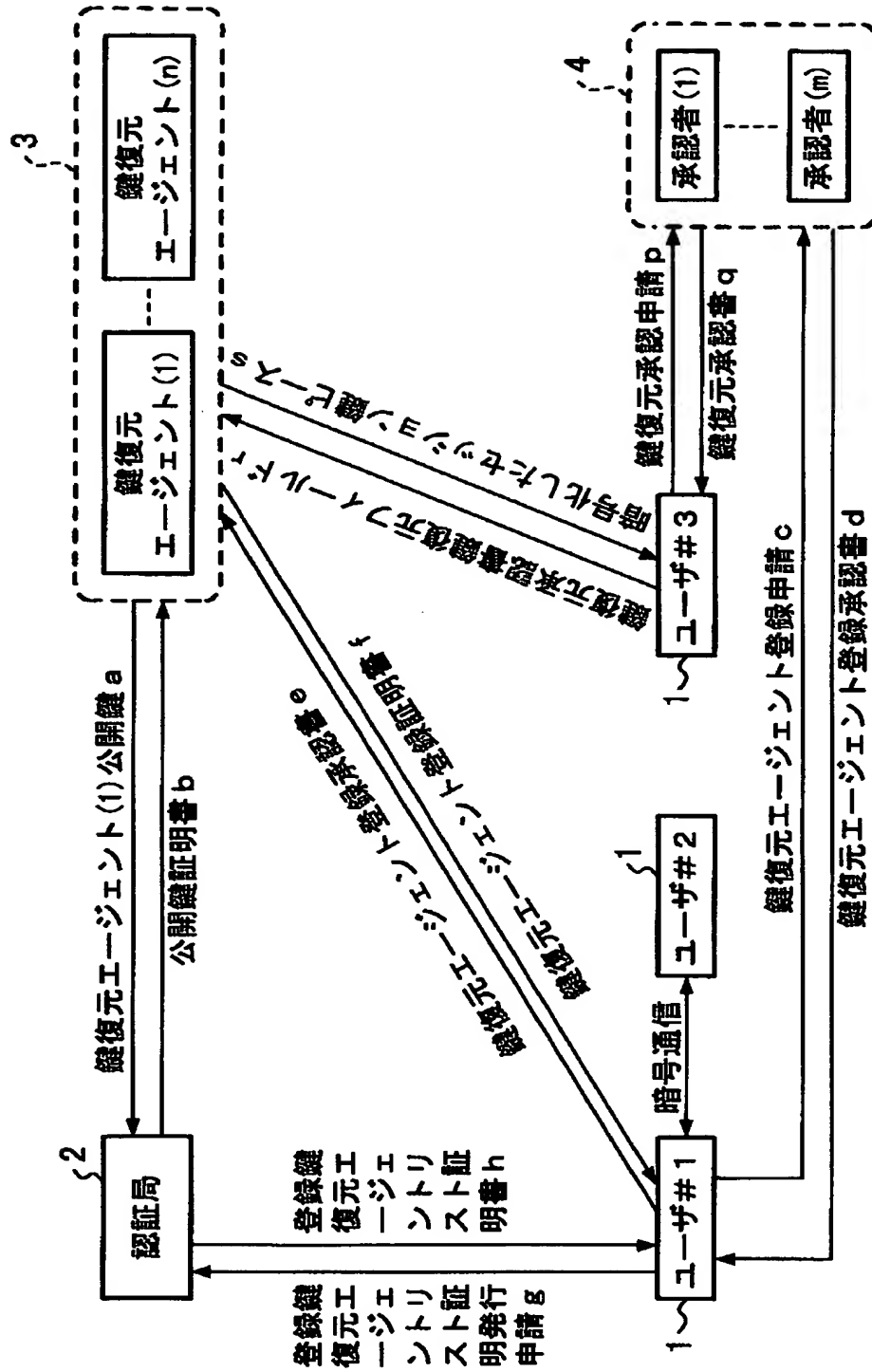
1 8 …プリンタ

1 9 …データバス

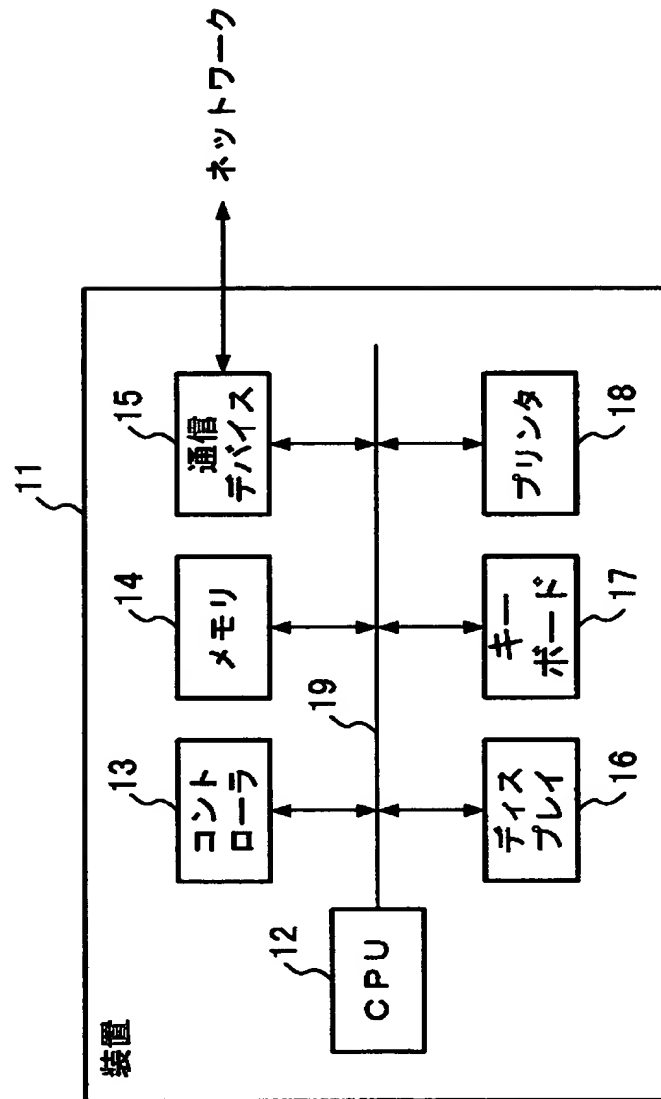
【書類名】

図面

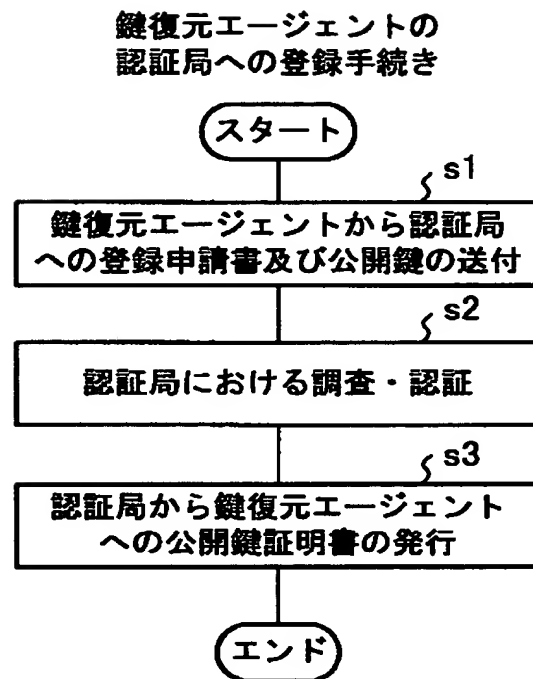
【図 1】



【図 2】

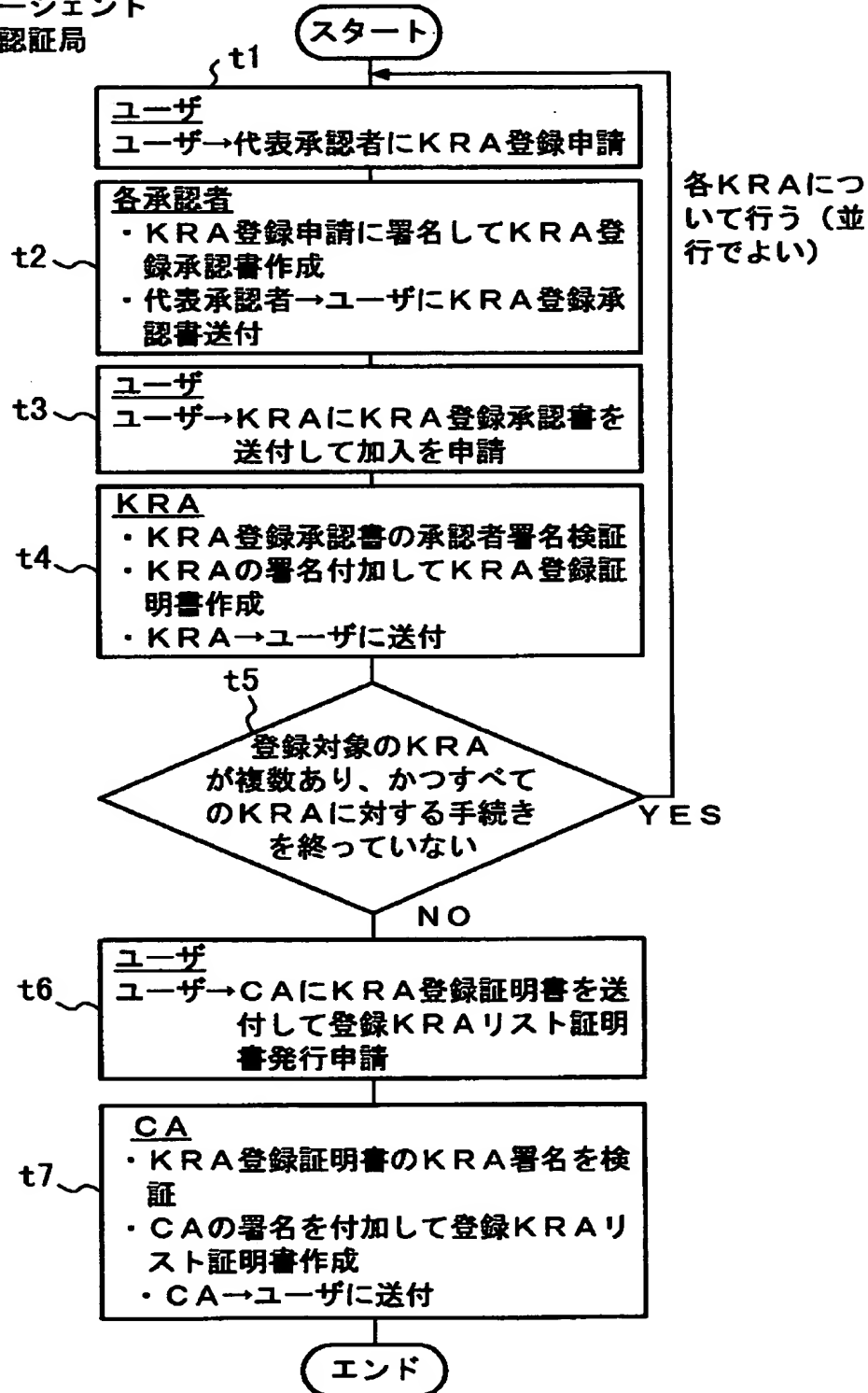


【図 3】



【図4】

KRA : ユーザのKRA登録手続き  
 鍵復元エージェント  
 CA : 認証局





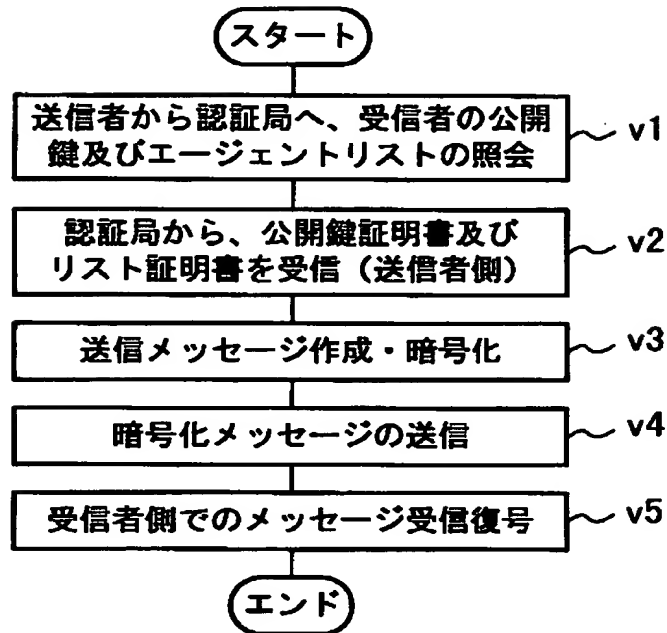
【図 5】

登録情報テーブル 21

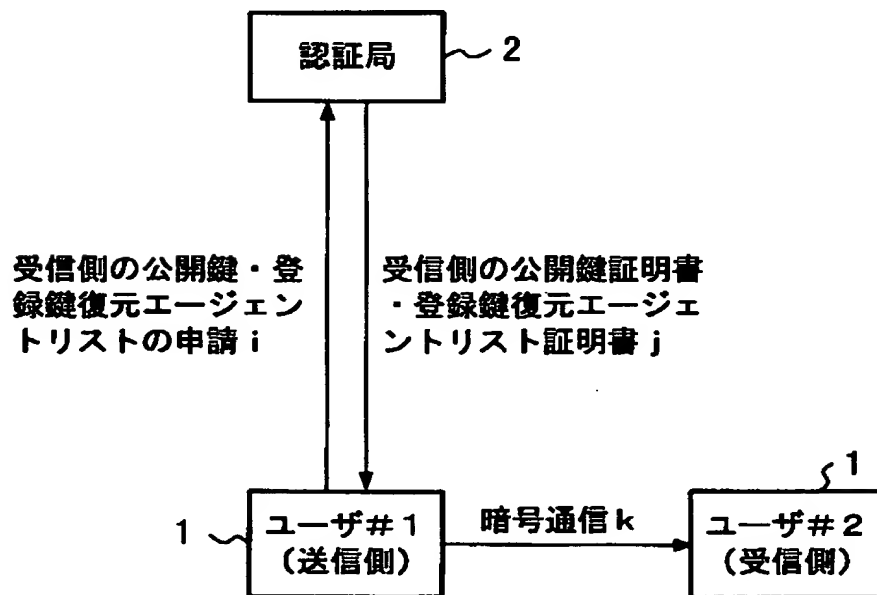
ユーザ、承認者、鍵復元エージェントの ID	認証局署名付公開鍵	ユーザが登録するエージェントリスト
ユーザ#1 ユーザ#2 ⋮ 承認者 $\alpha$ 承認者 $\beta$ ⋮ エージェントA エージェントB ⋮	○○○○ ×××× ⋮ △△△△ □□□□ ⋮ **** ▽▽▽▽ ⋮	A, B, C, B, D, G, H ⋮ なし なし ⋮ なし なし ⋮

【図 6】

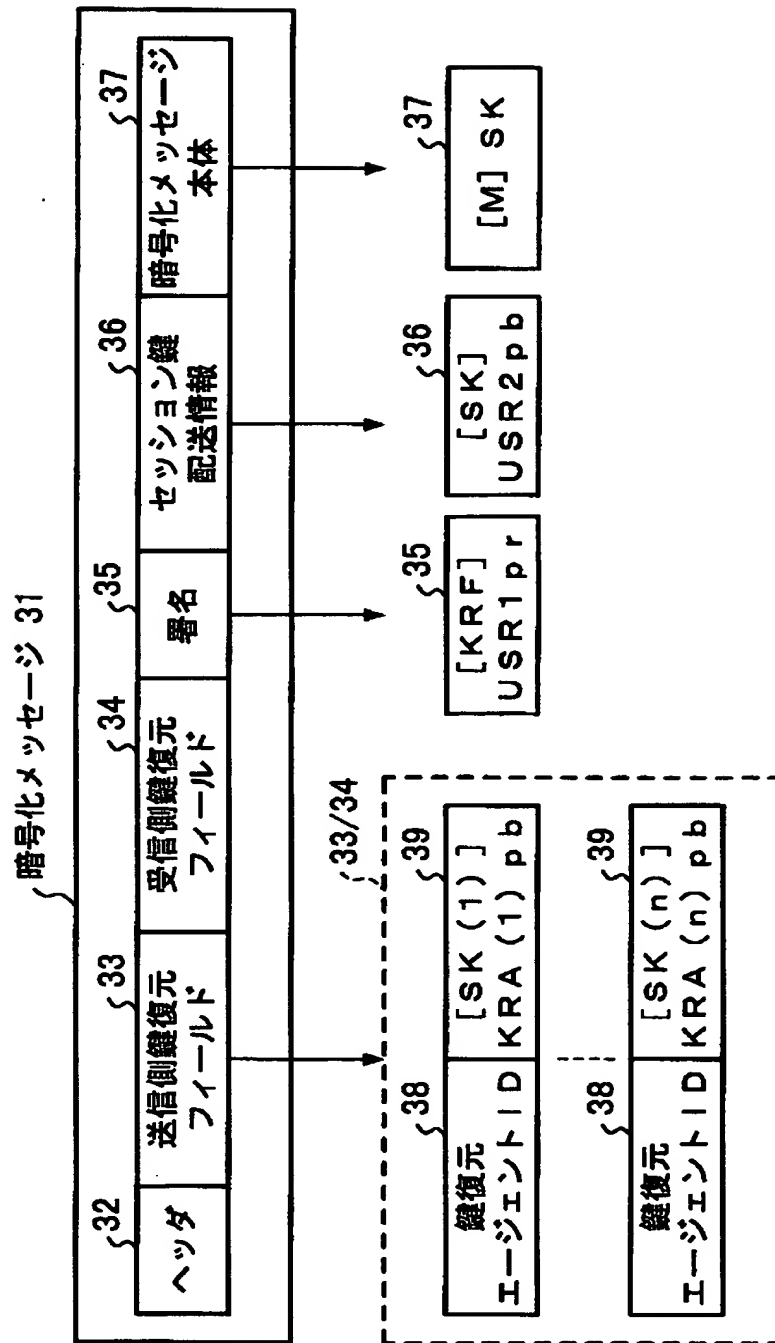
暗号化メッセージの送受信処理



【図 7】

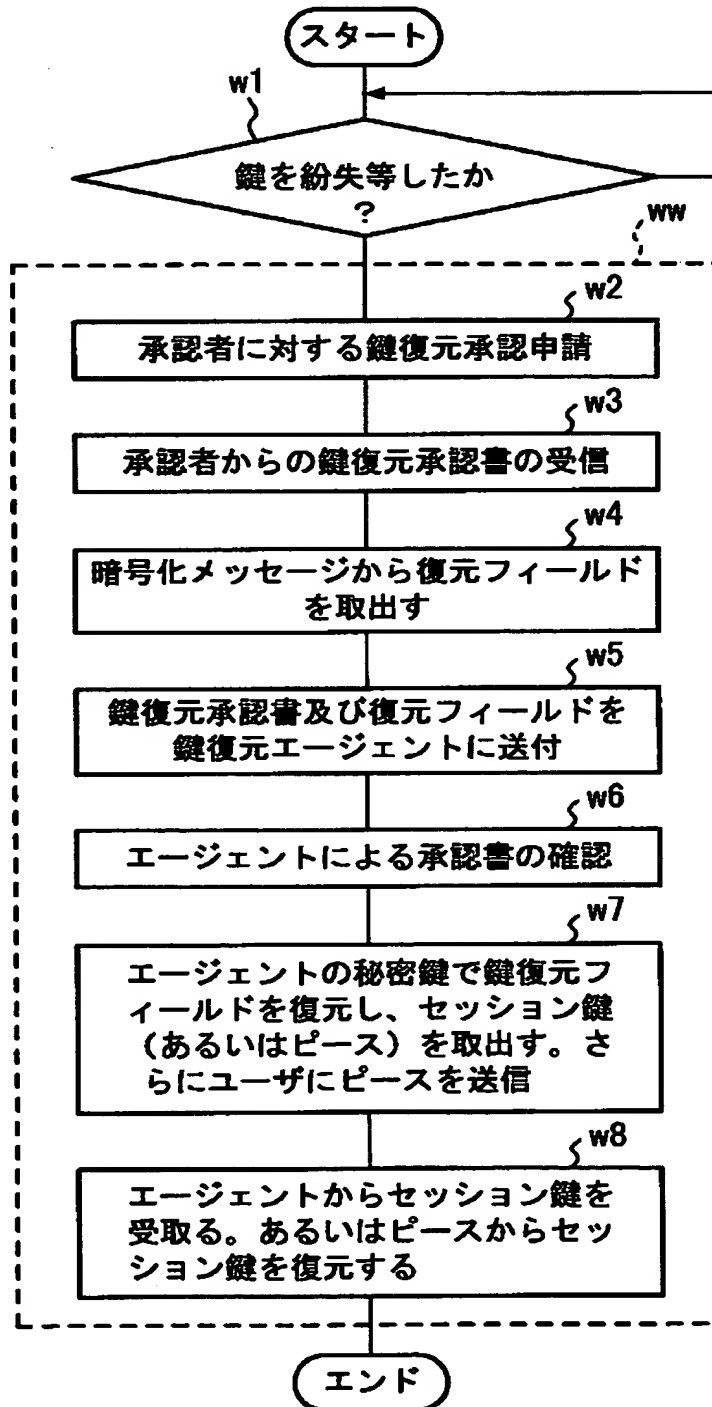


【図 8】

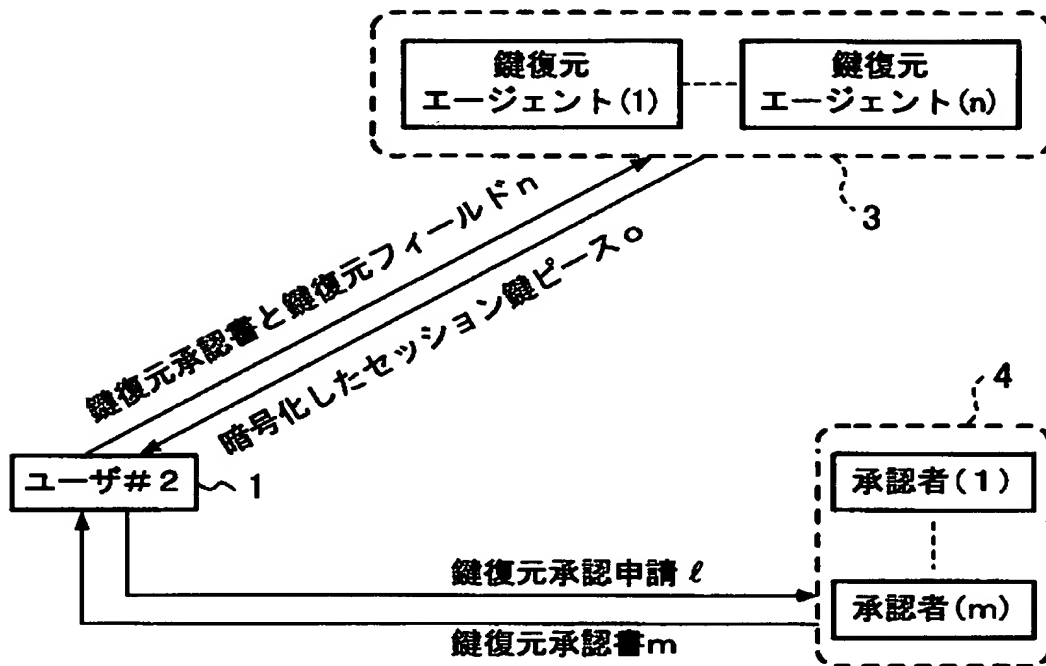


【図 9】

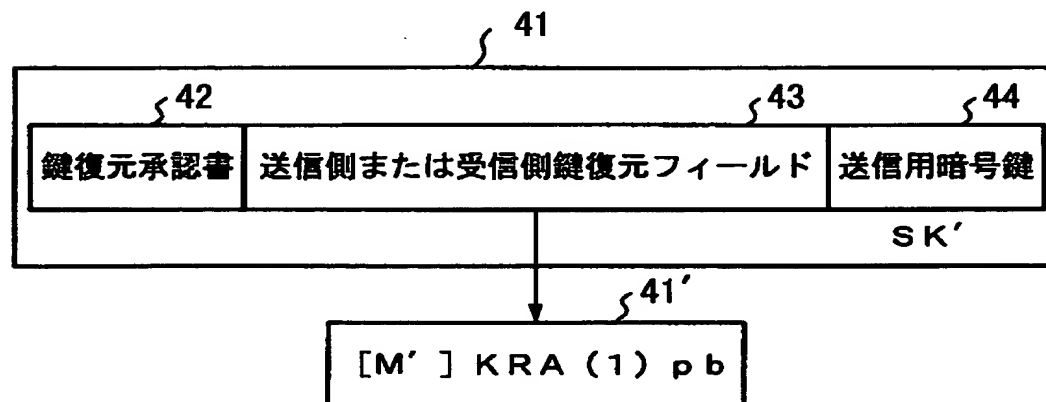
送信者又は受信者による鍵復元手続き



【図 10】

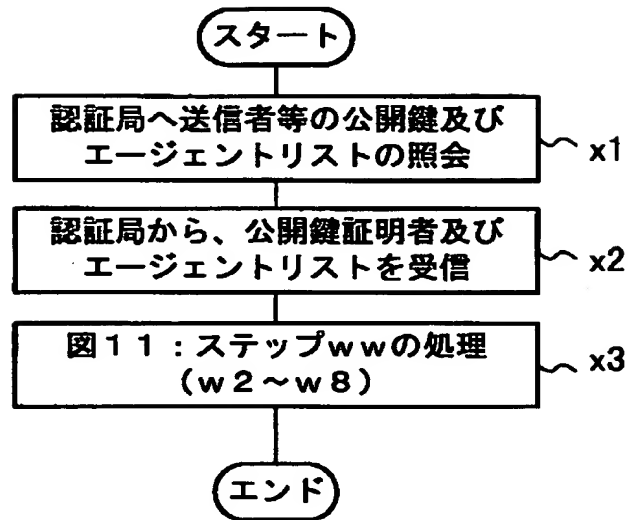


【図 11】

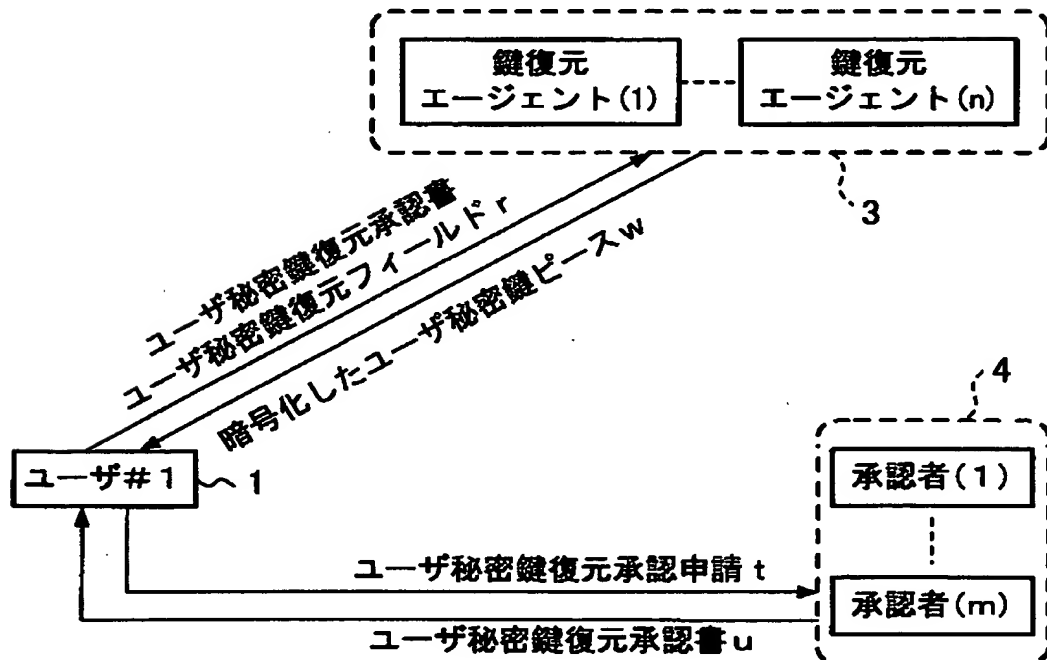


【図 12】

第3者による鍵復元手続き



【図 13】



【書類名】 要約書

【要約】

【課題】 鍵復号に関する権限集中やエージェントの結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【解決手段】 データ本体を暗号化して送信データ 31 に含め、当該送信データを受信者に送信する暗号装置であって、暗号化したデータ本体 37 を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データ 33 と、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データ 34 とを送信データに含める手段 11 を備えた暗号装置。

【選択図】 図 1

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000003078

【住所又は居所】 神奈川県川崎市幸区堀川町7番地

【氏名又は名称】 株式会社東芝

【代理人】 申請人

【識別番号】 100058479

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 鈴江 武彦

【選任した代理人】

【識別番号】 100084618

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 中村 誠

【選任した代理人】



【識別番号】 100070437  
【住所又は居所】 東京都千代田区霞が関3丁目7番2号 鈴築内外國  
特許法律事務所内  
【氏名又は名称】 河井 将次

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝